Securing a SaaS application with Developers

Who We Are

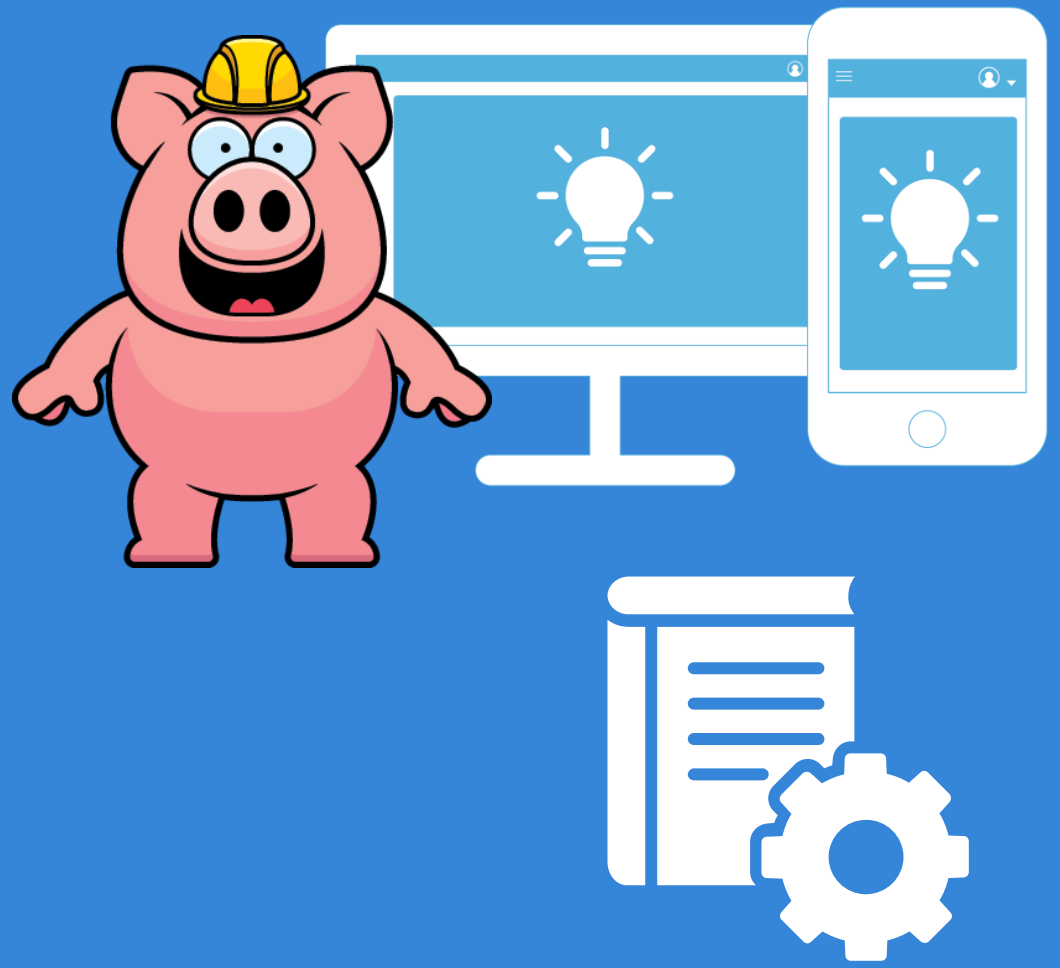
eBacon is a software as a service company that provides prevailing wage, payroll, and other solutions to construction companies in the United States. We've been around for 15 years and built a platform from the ground up to provide customers with the easiest solutions for their day-to-day needs.

Alex Kremer has worked at eBacon for 11 years, and currently heads up Development along with Security and Infrastructure.

eBacon

Our Application

We've had the privilege of building our application from the ground up. This has allowed us to create a lot of tools and flexibility for our customers. This also gives us a ton of power to customize where other systems cannot.



eBacon

Our Privacy and Security Concerns

Payroll companies are inside of a weird spot inside of the legal and compliance landscape. It is up to us to keep our customers data private, but most privacy laws (AKA California/Even EU) do not really contemplate employee level data, which is highly sensitive.

We are constantly responding to new threats that emerge in our industry, the My Payroll HR scandal, while not directly security related, indicates how payroll companies and money transfers can be used in ways they shouldn’t be.

Working with Developers

How does code get into a customer's hands?

Why Security and Development must connect

- Understanding risks and emerging threats together.
- Producing ways to best log and identify issues
- Educating on the latest and greatest
- Being proactive about your application

Misconceptions

- 'Hackers' are not writing code for systems that you use today. While some of them may of used their coding skills to get into things they shouldn't of, they don't have a deep knowledge of security.
- There are different types of developers in the universe (Frontend/backend) and their knowledge of security is only as good as the training they've received.
- Code isn't written in abstract 1 or 0 or assembly language anymore, a lot of what you use has very complex languages and tooling – Javascript and react as an example

Strategies for working with development

- Implementing security code reviews (On a smaller team it is important that you are reviewing or testing code)
- Working with development to setup correct logging.
- Knowing critical release dates and/or release cycle so you can be aware of what will change.
- Creating trainings and actively pentesting/reviewing code to these standards.
- Implementing tools that automate application security RASP (Runtime application self protection) WAF (Web application firewalls)
- Clearly communicating how attacks on other systems happened and identifying ways to improve your own.

Soft Skills

Keeping an organization safe requires a lot of technical skills, but it also requires even more soft skills such as :

- Writing
- Critical Thinking
- Reading
- Negotiation
- Vendor Management
- Interview Skills

Discussion/Open Questions